10.0 Equipment Management
10.04 MI-WIC Access *Effective Date:*

PURPOSE: To allow local agency users to access the MI-WIC Data System.

A. POLICY

1. Each MI-WIC data system user must read and sign the MI-WIC User Security and Confidentiality Agreement prior to requesting access to the MI-WIC application after they have applied for a Single Sign On (SSO) account. See Exhibit 10.04A MI-WIC User Security and Confidentiality Agreement.

2. Each user will have his/her own distinctive Single Sign On account.

3. To use the MI-WIC system, all local agency users must register in Michigan Department of Community Health's SSO website at https://sso.state.mi.us. If a user does not already have an SSO account they must register with SSO at the above address.
    a. The user must have an email address to create an SSO account.
    b. If the user does not have an agency email address, one can be created at www.yahoo.com or other free email source, or the user may use the WIC Coordinator's email address.

4. The WIC Coordinator shall be responsible for approving, denying and removing clinic staff not authorized to the MI-WIC system within the local agency. Only staff providing WIC services or direct supervision shall be granted access to the MI-WIC system.
    a. The WIC Coordinator shall be responsible for assigning the appropriate MI-WIC roles to access the MI-WIC system for each user.
    b. Denying or removing someone from the MI-WIC application does not remove the SSO User ID and password.

5. At the time of termination from a local WIC agency clinic, or a reassignment to another non-WIC program, all user roles must be removed from MI-WIC for that employee.

6. WIC Coordinators will alert the State when an employee is no longer employed in the local agency so the employee's SSO account can be terminated.

7. MI-WIC User Security and Confidentiality Agreements shall be kept current as long as the agency staff member has access to MI-WIC confidential information. The Agreement shall be updated if the employee's role changes within the WIC program. The Agreements shall be retained by the local agency for three years 150 days beyond employment by the local agency.

B. GUIDANCE

1. The SSO account registration process requires the user to provide Challenge/Response answers for later use if a password reset becomes necessary. The user should store the Challenge/Response answers in a safe place.

2. The top portion of the MI-WIC User Security and Confidentiality Agreement should be completed by the user with the following information:
    a. User Name
    b. Contact Phone Number
    c. Workplace Address or Location
    d. Fax Number
    e. Email Address
    f. User Signature and Date

3. The WIC Coordinator or designee will check the appropriate role permissions assigned to the user and sign and date the form.

Reference:
45 CFR 164.310
State of Michigan Computer Crime Law (Public Acts 1979-No.53)

Cross-Reference:
10.03 System Security

Exhibits:
10.04A MI-WIC User Security and Confidentiality Agreement